(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

**特開平9－134413**

(43)公開日　平成９年(1997)５月20日

| (51)Int.Cl.[6] | 識別記号 | 庁内整理番号 | ＦＩ | | 技術表示箇所 |
|---|---|---|---|---|---|
| Ｇ０６Ｋ　17/00 | | | Ｇ０６Ｋ　17/00 | Ｆ | |
| | | | | Ｅ | |
| Ｇ０９Ｃ　1/00 | ６１０ | 7259－5Ｊ | Ｇ０９Ｃ　1/00 | ６１０Ｄ | |
| | ６３０ | 7259－5Ｊ | | ６３０Ｃ | |
| Ｈ０４Ｌ　9/08 | | | Ｈ０４Ｌ　9/00 | ６０１Ｃ | |

審査請求　未請求　請求項の数３　ＯＬ　（全 14 頁）　最終頁に続く

(21)出願番号　特願平7－289871

(22)出願日　平成７年(1995)11月８日

(71)出願人　000134257
株式会社トーキン
宮城県仙台市太白区郡山６丁目７番１号

(72)発明者　三浦　融
宮城県仙台市太白区郡山六丁目７番１号
株式会社トーキン内

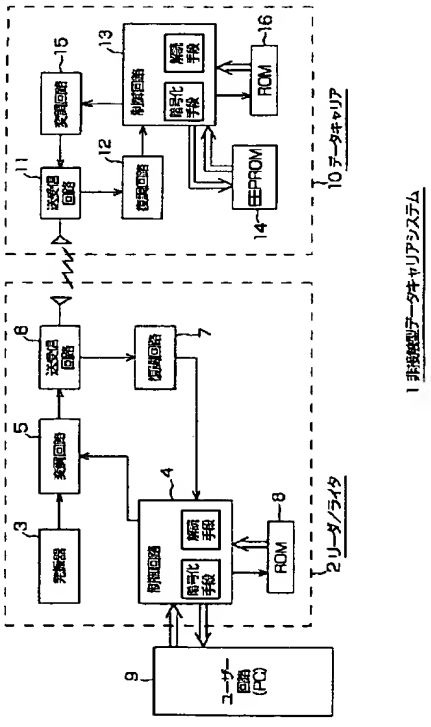
(74)代理人　弁理士　後藤　洋介　（外３名）

(54)【発明の名称】　非接触型データキャリアシステム

(57)【要約】

【課題】　一連の通信毎に異なった暗号化処理を行なえる非接触型データキャリアシステムを提供すること。

【解決手段】　暗号化処理を決定づけるキーデータを複数用意しておき、リーダ／ライタ２内のＲＯＭ８、及びデータキャリア１０内のＲＯＭ１６又はＥＥＰＲＯＭ１４に、該複数のキーデータからなるデータテーブルを記憶させておく。更に、通信開始時にリーダ／ライタ２及びデータキャリアの一方は、暗号化処理に用いるキーデータを決定し、該キーデータがデータテーブルの何処にあるのかを示す位置データを他方へ送信する。位置データを受信した該他方は、該位置データを用いてデータテーブルからキーデータを選択する。その後、一連の通信が終了するまで、リーダ／ライタ２及びデータキャリアの双方は、同じキーデータを用いた暗号化処理を行なう。



1

【特許請求の範囲】

【請求項１】　無線にてデータ通信を互いに行うデータキャリアとリーダ／ライタとからなり、

該データキャリアは、書き込み可能なデータメモリを有し、読み取り指令に基づいて該データメモリ中のデータを読み出し、データキャリア側の送信信号として前記リーダ／ライタに送信する機能と、前記リーダ／ライタからの送信信号を受信信号として受信する機能と、該受信信号中の読み取り命令に応じて前記読取り指令を送出する機能と、該受信信号中の書込みデータを前記データメモリ中に書込む機能とを有しており、

前記リーダ／ライタは、前記データキャリア側の送信信号を受信して前記データメモリ中のデータを取得する機能と、前記データメモリ中のデータを読み取るべき前記読み取り命令あるいは、前記データメモリ中に書込むべき前記書込みデータを前記リーダ／ライタ側の送信信号として送信する機能とを有してなる非接触型データキャリアシステムにおいて、

前記リーダ／ライタおよび前記データキャリアのそれぞれは、

両者間の通信データを暗号化処理するための複数個の異なる暗号化キーデータをテーブルとして記憶するための暗号化キーデータメモリと、

通信開始時に該暗号化キーデータの中から特定の一つを特定暗号化キーデータとして選択し、送信データを該特定暗号化キーデータに基づき暗号化する暗号化手段と、受信信号を前記特定の暗号化キーデータに基づいて解読する解読手段とを有し、

これにより、一連の通信毎に、異なる暗号化処理を選択できることを特徴とする非接触型データキャリアシステム。

【請求項２】　請求項１の非接触型データキャリアシステムにおいて、

前記暗号化キーデータのテーブルは、各暗号化キーデータに固有のキーコードを有しており、

前記データキャリアは、前記リーダ／ライタ側送信信号を受信したときに、前記特定暗号化キーデータを選択する手段と、該特定暗号化キーデータのキーコードをキャリア側送信データの一つとして、前記リーダ／ライタに通知する手段とを有することを特徴とする非接触型データキャリアシステム。

【請求項３】　請求項１の非接触型データキャリアシステムにおいて、

前記暗号化キーデータのテーブルは、各暗号化キーデータに固有のキーコードを有しており、

前記リーダ／ライタは、その送信開始時に、前記特定暗号化キーデータを選択する手段と、該特定暗号化キーデータのキーコードをリーダ／ライタ側送信データの一つとして、前記リーダ／ライタに通知する手段とを有することを特徴とする非接触型データキャリアシステム。

2

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、読み出し及び書き換え可能なメモリと通信機能とを内蔵したＩＣカード等からなりＩＤカード・定期券・プリペイドカード等に使用されるデータキャリアと、通信機能を有するリーダ／ライタとからなり、電磁結合方式、電磁誘導方式、光方式、電波方式等の非接触によるデータ通信によって、リーダ／ライタからデータキャリアに内蔵されたメモリへのデータの読みだし及び書き換えが可能である非接触型データキャリアシステムに関する。

【０００２】

【従来の技術】現在、非接触型データキャリアシステムのデータキャリアとして一般的に使用されているものには、ＣＰＵ・マスクＲＯＭ・ＲＡＭ・各種周辺素子等に電気的に書き換え可能なＥＥＰＲＯＭ（Ｅｌｅｃｔｒｉｃａｌｌｙ　ＥｒａｓａｂｌｅＰｒｏｇｒａｍａｂｌｅ　Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｌｙ）または書き換えのできないＰＲＯＭを加えて構成した専用ＩＣチップを内蔵したものと、ゲートアレイによりロジック回路を構成した専用ＩＣにＥＥＰＲＯＭまたはＰＲＯＭを組み合わせて内蔵したもの等があり、塩化ビニル、樹脂モールド等により密封される。

【０００３】これらのデータキャリアを有する非接触型データキャリアシステムは、外部とのデータ入出力用接続端子を有さず、電磁結合方式・電磁誘導方式・光方式・電波方式等により、非接触でリーダ／ライタとデータキャリア間のデータ通信を行い、リーダ／ライタからデータキャリア内のメモリに記憶されたデータの読みだし或いは書き換えを行えるようになっているため、水・塵・静電気等による影響がなく耐環境性に優れている。

【０００４】また、これらの非接触型データキャリアシステムのデータキャリアは、接続端子又は磁気ヘッドに接触させる必要がある従来の接触型ＩＣカード或いは磁気カードのように、リーダ／ライタへ挿入する手間もなく、専用のリーダ／ライタにかざすようにするだけで動作するため、操作性が向上している。

【０００５】

【発明が解決しようとする課題】ここで、非接触型データキャリアシステムは、ＩＤデータ・金銭データ等のデータを取り扱うため、当然のことながら、セキュリティが要求されることとなる。従って、非接触によるデータ通信には、そのデータ通信方式、データの変調／復調方式、データの構成など、様々な方法が採用されており、それらがセキュリティの向上に貢献している。

【０００６】しかしながら、リーダ／ライタとデータキャリア間の双方の通信データの内容が解読困難であったとしても、通信信号自体、例えば電磁波や光などの変調信号を、通信を行っているリーダ／ライタ及びデータキャリア以外のコイルや受光素子等を用いて捕らえること

は容易である。このようにして、捕らえた信号と同一の信号をリーダ／ライタやデータキャリアに対して送信されると、誤動作をしてしまう可能性がある。また、このようなことが不正目的に利用されてしまうかもしれないことは、十分に予想されることである。

【０００７】本発明は、このような問題点を解決すべくなされたもので、一連の通信開始時毎に、暗号化処理を決定づけるデータをキーデータとして、リーダ／ライタ又はデータキャリアのどちらかで決定する手段、リーダ／ライタ又はデータキャリアのどちらか一方で決定されたキーデータを、他方に通知する手段とを有し、一連の処理毎にキーデータを変更することで、常に暗号化処理が変化し、不正操作による誤動作を防止し、セキュリティを向上させる非接触データキャリアシステムを提供するものである。

【０００８】

【課題を解決するための手段】即ち、本発明によれば、無線にてデータ通信を互いに行うデータキャリアとリーダ／ライタとからなり、該データキャリアは、書き込み可能なデータメモリを有し、読み取り指令に基づいて該データメモリ中のデータを読み出し、データキャリア側の送信信号として前記リーダ／ライタに送信する機能と、前記リーダ／ライタからの送信信号を受信信号として受信する機能と、該受信信号中の読み取り命令に応じて前記読取り指令を送出する機能と、該受信信号中の書込みデータを前記データメモリ中に書込む機能とを有しており、前記リーダ／ライタは、前記データキャリア側の送信信号を受信して前記データメモリ中のデータを取得する機能と、前記データメモリ中のデータを読み取るべき前記読み取り命令あるいは、前記データメモリ中に書込むべき前記書込みデータを前記リーダ／ライタ側の送信信号として送信する機能とを有してなる非接触型データキャリアシステムにおいて、前記リーダ／ライタおよび前記データキャリアのそれぞれは、両者間の通信データを暗号化処理するための複数個の異なる暗号化キーデータをテーブルとして記憶するための暗号化キーデータメモリと、通信開始時に該暗号化キーデータの中から特定の一つを特定暗号化キーデータとして選択し、送信データを該特定暗号化キーデータに基づき暗号化する暗号化手段と、受信信号を前記特定の暗号化キーデータに基づいて解読する解読手段と、を有し、これにより、一連の通信毎に、異なる暗号化処理を選択できることを特徴とする非接触型データキャリアシステムが得られる。

【０００９】また、本発明によれば、前記非接触型データキャリアシステムにおいて、前記暗号化キーデータのテーブルは、各暗号化キーデータに固有のキーコードを有しており、前記データキャリアは、前記リーダ／ライタ側送信信号を受信したときに、前記特定暗号化キーデータを選択する手段と、該特定暗号化キーデータのキーコードをキャリア側送信データの一つとして、前記リーダ／ライタに通知する手段とを有することを特徴とする非接触型データキャリアシステムが得られる。

【００１０】更に、本発明によれば、前記非接触型データキャリアシステムにおいて、前記暗号化キーデータのテーブルは、各暗号化キーデータに固有のキーコードを有しており、前記リーダ／ライタは、その送信開始時に、前記特定暗号化キーデータを選択する手段と、該特定暗号化キーデータのキーコードをリーダ／ライタ側送信データの一つとして、前記リーダ／ライタに通知する手段とを有することを特徴とする非接触型データキャリアシステムが得られる。

【００１１】

【発明の実施の形態】以下に、本発明の実施の形態を図面を用いて説明する。

【００1-2】本発明の実施の形態の非接触型データキャリアシステム１は、図１に示す様な、リーダ／ライタ２及びデータキャリア１０から構成されている。

【００１３】リーダ／ライタ２において、発振器３は、一定の周波数の信号を変調回路５へ送出し、また、ＣＰＵを中心に構成された制御回路４は、データキャリア１０のＥＥＰＲＯＭ１４に対するデータの読み出し或いは書き込みなどの要求を示すコマンドコード及びデータからなるコマンド電文を作成し、その作成したコマンド電文を変調回路５へ送出する。変調回路５は、発振器３より受けた信号を用いて、制御回路４から受けたコマンド電文を変調し、送受信回路６へ送出する。送受信回路６は、変調回路５から受けたコマンド電文をデータキャリア１０へ送信する一方、データキャリア１０から送信されてきた後述するレスポンス電文を受信し、その受信したレスポンス電文を復調回路７へ送出する。復調回路７は、送受信回路６から受けたレスポンス電文を復調し、制御回路４へ送出する。

【００１４】一方、データキャリア１０において、送受信回路１１は、リーダ／ライタ２から送信されてきたコマンド電文を受信し、復調回路１２へ送出する。復調回路１２は、送受信回路１１から受けたコマンド電文を復調し、制御回路１３へ送出する。制御回路１３は、復調回路１２により復調されたコマンド電文に従い、ＥＥＰＲＯＭ１４に対して読み込み或いは書き込みを行なうと共に、レスポンスコード及びデータからなるレスポンス電文を作成し、その作成したレスポンス電文を変調回路１５へ送出する。変調回路１５は、制御回路１３から受けたレスポンス電文を変調し、送受信回路１１へ送出する。送受信回路１１は、変調回路１５から受けた変調されたレスポンス電文をリーダ／ライタ２へ送信する。

【００１５】また、ユーザー回路９は、リーダ／ライタ２の制御を行なうものであり、本発明の実施の形態では、一例として、パーソナルコンピュータ（ＰＣ）を使用した。更に、リーダ／ライタ２内のＲＯＭ８及びデータキャリア１０内のＲＯＭ１６は、双方とも、それぞれ

の動作を制御するプログラムを記憶している。

【００１６】ここで、本発明の実施の形態においては、リーダ／ライタ２内のＲＯＭ８及びデータキャリア１０内のＲＯＭ１６に、更に、暗号化処理のためのプログラム、及び暗号解読のためのプログラム、並びに、後述する様に、暗号化処理を決定づけるデータテーブルを記憶させてある。リーダ／ライタ２及びデータキャリア１０は、これらのプログラムをそれぞれの制御回路が実行することにより、暗号化処理をソフト的に行なっている。

【００１７】尚、上記のリーダ／ライタ２内のＲＯＭ８及びデータキャリア１０内のＲＯＭ１６に記憶されている暗号化処理のためのプログラムと、及び暗号解読のためのプログラムと、並びに暗号化処理を決定づけるデータテーブルと、それらのプログラムを実行している制御回路の機能を持つ様な回路又はそれらの内の一部の機能を実行する様な回路を別に構成し、暗号化処理をハード的に行なってもよい。

【００１８】次に、本発明の実施の形態における暗号化処理について説明する。

【００１９】まず、本発明の実施の形態の非接触型データキャリアシステム１において、リーダ／ライタ２とデータキャリア１０との間の通信で使用される暗号化処理のアルゴリズムは、予め、決定されている。ここで、簡単な例として、ｙ＝（ｘ　ＸＯＲ　ａ）＋ｂという関数を用いて暗号化処理を説明する。尚、ｙは暗号化処理した結果の１バイトデータを、ｘは暗号化処理する前の１バイトデータを、ａ及びｂはこの暗号化処理を決定づける各１バイトのキーデータを示すものである。暗号化処理は、この式を用いて、単純な排他的論理和（ＸＯＲ）と加算によって行なわれている。尚、この計算は、１バイト毎に行なわれ、桁上げが生じた場合には無視するものとする。暗号解読処理は、暗号化処理に用いた式を逆に計算して行なえばよく、ｘ＝（ｙ－ｂ）　ＸＯＲ　ａとなる。

【００２０】これらの暗号化処理を決定づけるのは、ａ及びｂといったキーデータである。本発明の非接触型データキャリアシステム１においては、これらのキーデータを複数組み用意し、リーダライタ２内のＲＯＭ８、及びデータキャリア１０内のＲＯＭ１６或いはＥＥＰＲＯＭ１４に、図２に示す様な、同一のデータテーブルとして記憶させてある。ここで、図２において、ｎとあるのは、各キーデータのコード、即ちキーコードであり、この実施の形態においては、どのキーデータがデータテーブルの何番目にあるのかを示す位置データである。

【００２１】データキャリア１０がリーダ／ライタ２との通信領域に入り、通信によりお互いの存在が確認された時に、リーダ／ライタ２及びデータキャリア１０のいずれかにおいて、前述のａ及びｂといったキーデータを無作為に選択決定する。更に、リーダ／ライタ２及びデータキャリア１０の一方は、キーデータを選択決定すると、その選択決定されたキーデータのデータテーブルにおける位置を示す位置データを、通信により他方に通知する。

【００２２】リーダ／ライタ２及びデータキャリア１０の一方が、他方にどのキーデータを選択決定したのかを示す位置データを他方に通知すると、双方ともが同一のキーデータを認識することができるため、これ以後の通信は、選択決定されたキーデータ、即ちａ及びｂを用いて、リーダ／ライタ２とデータキャリア１０との間で送受信されるデータの内容に対し、それぞれ暗号化処理及び暗号解読処理を行ない、暗号化処理されたデータによって行なわれることになる。尚、ここで、キーデータは、一連の通信が終了するまで同一のものを用いることとする。

【００２３】これにより、通信自体が暗号化されるため、解読が困難になることに加え、一連の通信毎に暗号化を決定づけるキーデータが変わるため、不正目的により以前に捕らえられた通信信号を真似た信号が外部から送出されてきたとしても、次の一連の通信では内容を正しく解読することができないため、誤動作を防げることになる。また、暗号化処理を決定づける選択決定されたキーデータは、通信上に直接現れることがないため、暗号化処理されたデータの解読を更に困難なものとしている。

【００２４】以上に説明してきたことは、以下に示す第１及び第２の実施の形態について共通のことである。

【００２５】（第１の実施の形態）以下に、第１の実施の形態の非接触型データキャリアシステム１の動作を図３乃至図６を用いて説明する。

【００２６】第１の実施の形態の非接触型データキャリアシステム１は、データキャリア１０が暗号化を決定づけるキーデータを選択決定し、その選択決定されたキーデータのデータテーブルにおける位置を示す位置データをリーダ／ライタ２に通知することにより暗号化処理を行なったデータの通信を可能とするものである。

【００２７】まず、図３を用いてリーダ／ライタ２の動作を説明する。リーダ／ライタ２は、図５に示されるコマンド電文フォーマットに従って、起動コマンドをコマンドコードにセットし、一定の周期で起動コマンドを含むコマンド電文を送信している（Ｓ１０１）。ここで、図５中のＳＴＸ（０２）は、コマンド電文開始コードを、ＥＴＸ（０３）は、コマンド電文の終了コードを意味し、ＢＣＣ(Block Check Character) は、ＳＴＸの次からＥＴＸまでの排他的論理和（ＸＯＲ）の計算結果をセットすることを意味する。次に、リーダ／ライタ２は、データキャリア１０が通信可能な領域にあれば、データキャリア１０がこのコマンド電文に対するレスポンス電文を送信してくるため、このレスポンス電文の受信の有無を判定する（Ｓ１０２）。リーダ／ライタ２は、データキャリア１０からのレスポンス電文を受信しない

限り、ステップＳ１０１へ戻り、コマンド電文を送信し続ける。データキャリア１０からのレスポンス電文を受信すると、そのレスポンス電文には、後述する様に、データキャリア１０の選択決定したキーデータのデータテーブルにおける位置を示す位置データが含まれているため、リーダ／ライタ２は位置データを取得する（Ｓ１０３）ことができる。リーダ／ライタ２は、位置データを取得すると、それに基づいて、複数のキーデータからなるデータテーブルから、データキャリア１０の選択決定したキーデータを選択する（Ｓ１０４）。

【００２８】リーダ／ライタ２は、これ以降、一連の通信が終了するまで、このキーデータを用いて暗号化処理された電文にてデータキャリア１０との通信を行なう。

【００２９】リーダ／ライタ２は、ステップＳ１０４において選択されたキーデータを用いて、コマンド電文フォーマットに従ったコマンド電文のコマンドコードとデータに、暗号化手段により、暗号化処理を施して暗号化されたコマンド電文を作成し、データキャリア１０に暗号化されたコマンド電文を送信する（Ｓ１０５）。データキャリア１０がこのコマンド電文を受信すると、このコマンド電文に対する暗号化されたレスポンス電文を送信してくるため、リーダ／ライタ２は、このレスポンス電文の受信の有無を判定する（Ｓ１０６）。リーダ／ライタ２は、データキャリア１０からのレスポンス電文を受信しない限り、ステップＳ１０５へ戻り、暗号化されたコマンド電文をデータキャリア１０に送信し続ける。リーダ／ライタ２は、暗号化されたレスポンス電文を受信すると、暗号解読手段により、暗号化されたレスポンス電文を解読する（Ｓ１０７）。その後、通信を終了するかどうかを判定し（Ｓ１０８）、通信を終了しない場合は、ステップＳ１０５に戻り、更に一連の動作を繰り返す。通信を終了する場合、リーダ／ライタ２は、通信終了を意味するコマンドコードを含むコマンド電文に対し、暗号化手段により、暗号化処理を施して暗号化されたコマンド電文を作成し、データキャリア１０に暗号化された通信終了を意味するコマンド電文を送信する（Ｓ１０９）。データキャリア１０がこのコマンド電文を受信すると、このコマンド電文に対する暗号化されたレスポンス電文を送信してくるため、リーダ／ライタ２は、このレスポンス電文の受信の有無を判定する（Ｓ１１０）。リーダ／ライタ２は、データキャリア１０からのレスポンス電文を受信しない限り、ステップＳ１０９へ戻り、暗号化されたコマンド電文をデータキャリア１０に送信し続ける。リーダ／ライタ２は、暗号化されたレスポンス電文を受信すると、暗号解読手段により、暗号化されたレスポンス電文を解読し（Ｓ１１１）、一連の通信を終了する。

【００３０】次に、図４を用いて、データキャリア１０の動作について説明する。データキャリア１０は、電源（図示せず）から供給を受けると、位置データの値ｎに初期値として０をセットする（Ｓ２０１）。その後、リーダ／ライタ２からの起動コマンドを含むコマンド電文を受信するまで、一定の周期で起動コマンドを含むコマンド電文を受信したかどうかの判定を行なう（Ｓ２０２）。データキャリア１０は、このコマンド電文を受信しない限り、位置データの値ｎに１を加え（Ｓ２０３）、ステップＳ２０２へ戻る。ここで、本実施の形態において用いられるデータテーブルは、図２に示されているものであるため、位置データに上限がある。したがって、ステップＳ２０３において、１を加えた後、更に、ｎの値が０Ｆｈを越えた場合、ｎの値から１０ｈを引くこととしている。次に、データキャリア１０は、リーダ／ライタ２からの起動コマンドを含むコマンド電文を受信すると、ｎの値から、位置データの決定を行ない（Ｓ２０４）、その決定した位置データに従い、データテーブルからキーデータを選択決定する（Ｓ２０５）。その後、データキャリア１０は、図６のレスポンス電文フォーマットに従い、レスポンスコードと位置データの値をセットしたレスポンス電文を作成し、作成したレスポンス電文をリーダ／ライタ２へ送信する（Ｓ２０６）。ここで、図６に示されるレスポンス電文中のＳＴＸ（０２）、ＥＴＸ（０３）、ＢＣＣは、前述したコマンド電文におけるものと同じ意味を持つものである。

【００３１】データキャリア１０は、これ以降、一連の通信が終了するまで、このキーデータを用いて暗号化処理された電文にてリーダ／ライタ２との通信を行なう。

【００３２】ここで、図２のデータテーブルを用いて、暗号化処理についての説明をする。暗号化処理は、前述したコマンド電文においてはコマンドコードとデータに対して、レスポンス電文においては、レスポンスコードとデータに対して行なわれる。例えば、データキャリア１０が決定した位置データが８であったとすると、ａとｂからなるキーデータは、それぞれａ＝７１ｈ、ｂ＝Ｆ２ｈとなる。また、コマンドコード又はレスポンスコードが３１、データが５５であったとすると、暗号化処理を施される前のコマンド電文又はレスポンス電文は、０２　３１　５５０３　６７　となる。このコマンド電文又はレスポンス電文の、コマンドコード或いはレスポンスコード、及びデータに対して、ｙ＝（ｘ　ＸＯＲ　７１）＋Ｆ２の暗号化処理が行なわれると、０２　３２　１６　０３　２７　となる。逆に、暗号解読処理は、ｘ＝（ｙ－Ｆ２）　ＸＯＲ　７１の式にて行なわれる。

【００３３】データキャリア１０は、リーダ／ライタ２から、暗号化処理されたコマンド電文を受信すると（Ｓ２０７）、暗号化処理されたコマンド電文に対し、選択決定したキーデータを用いて暗号解読処理を行ない、暗号化処理されたコマンド電文を解読する（Ｓ２０８）。次に、データキャリア１０は、暗号解読されたコマンド電文が通信終了を指示するものかどうかを判定する（Ｓ２０９）。コマンド電文が通信終了を指示するものでな

い場合、データキャリア１０は、暗号化処理したレスポンス電文をリーダ／ライタ２へ送信し（Ｓ２１０）、ステップＳ２０７へ戻り、次の暗号化処理されたコマンド電文を受信するまで待機をする。ステップＳ２０９において、暗号解読されたコマンド電文が通信終了を指示するものであった場合、データキャリア１０は、そのコマンド電文に対応する暗号化処理されたレスポンス電文を作成し、リーダ／ライタ２へ送信し（Ｓ２１１）、一連の通信を終了する。

【００３４】このようにして、本発明の第１の実施の形態におけるデータキャリア１０及びリーダ／ライタ２からなる非接触型データキャリアシステム１は、一連の通信毎に、暗号化処理に用いるキーデータを変えることができ、各通信毎に異なる暗号化処理を行なうことが可能となった。

【００３５】（第２の実施の形態）次に、第２の実施の形態の非接触型データキャリアシステム１の動作を図５乃至図８を用いて説明する。

【００３６】第２の実施の形態の非接触型データキャリアシステム１は、第１の実施の形態とは異なり、リーダ／ライタ２が暗号化を決定づけるキーデータを選択決定し、その選択決定されたキーデータのデータテーブルにおける位置を示す位置データをデータキャリア１０に通知することにより暗号化処理を行なったデータの通信を可能とするものである。また、暗号化処理及び暗号解読処理は、第１の実施の形態と同じものとした。

【００３７】まず、図７を用いてリーダ／ライタ２の動作を説明する。リーダ／ライタ２は、位置データの値ｎに初期値０をセットする（Ｓ３０１）。次に、リーダ／ライタ２は、図５に示されるコマンド電文フォーマットに従って、起動コマンドをコマンドコードにセットし、一定の周期で起動コマンドを含むコマンド電文を送信する（Ｓ３０２）。次に、リーダ／ライタ２は、データキャリア１０が通信可能な領域にあれば、データキャリア１０がこのコマンド電文に対するレスポンス電文を送信してくるため、このレスポンス電文の受信の有無を判定する（Ｓ３０３）。リーダ／ライタ２は、データキャリア１０からのレスポンス電文を受信しなかった場合、位置データの値ｎに１を加え（Ｓ３０４）、ステップＳ２０２へ戻り、コマンド電文を送信し続ける。ここで、ｎが０Ｆを越えた場合は、第１の実施の形態のデータキャリア１０のステップＳ２０３における動作と同じ動作を行なう。

【００３８】データキャリア１０からのレスポンス電文を受信すると、リーダ／ライタ２は、ｎの値から位置データを決定し（Ｓ３０５）、その位置データに従い、データテーブルから暗号化処理に用いるキーデータを決定する（Ｓ３０５）。その後、リーダ／ライタ２は、位置データを含むコマンド電文をデータキャリア１０に送信し（Ｓ３０７）、データキャリア１０からのレスポンス電文を受信したかどうかを判定する（Ｓ３０８）。ステップＳ３０８において、データキャリア１０からのレスポンス電文が受信されなかった場合、リーダ／ライタ２は、ステップＳ３０７に戻り、再び位置データを含むコマンド電文をデータキャリア１０に送信する。

【００３９】一方、ステップＳ３０８において、データキャリア１０からのレスポンス電文を受信した場合、リーダ／ライタ２は、これ以降、一連の通信が終了するまで、選択決定したキーデータを用いて暗号化処理された電文にてデータキャリア１０との通信を行なう。

【００４０】ステップＳ３０８において、データキャリア１０からのレスポンス電文を受信すると、リーダ／ライタ２は、選択決定したキーデータを用いて、コマンド電文フォーマットに従ったコマンド電文のコマンドコードとデータに、暗号化手段により、暗号化処理を施して暗号化されたコマンド電文を作成し、データキャリア１０に暗号化されたコマンド電文を送信する（Ｓ３０９）。データキャリア１０がこのコマンド電文を受信すると、このコマンド電文に対する暗号化されたレスポンス電文を送信してくるため、リーダ／ライタ２は、このレスポンス電文の受信の有無を判定する（Ｓ３１０）。リーダ／ライタ２は、データキャリア１０からのレスポンス電文を受信しない限り、ステップＳ３０９へ戻り、暗号化されたコマンド電文をデータキャリア１０に送信し続ける。リーダ／ライタ２は、暗号化されたレスポンス電文を受信すると、暗号解読手段により、暗号化されたレスポンス電文を解読する（Ｓ３１１）。その後、通信を終了するかどうかを判定し（Ｓ３１２）、通信を終了しない場合は、ステップＳ３０９に戻り、更に一連の動作を繰り返す。通信を終了する場合、リーダ／ライタ２は、通信終了を意味するコマンドコードを含むコマンド電文に対し、暗号化手段により、暗号化処理を施して暗号化されたコマンド電文を作成し、データキャリア１０に暗号化された通信終了を意味するコマンド電文を送信する（Ｓ３１３）。データキャリア１０がこのコマンド電文を受信すると、このコマンド電文に対する暗号化されたレスポンス電文を送信してくるため、リーダ／ライタ２は、このレスポンス電文の受信の有無を判定する（Ｓ３１４）。リーダ／ライタ２は、データキャリア１０からのレスポンス電文を受信しない限り、ステップＳ３１３へ戻り、暗号化されたコマンド電文をデータキャリア１０に送信し続ける。リーダ／ライタ２は、暗号化されたレスポンス電文を受信すると、暗号解読手段により、暗号化されたレスポンス電文を解読し（Ｓ３１５）、一連の通信を終了する。

【００４１】次に、図８を用いて、データキャリア１０の動作について説明する。データキャリア１０は、電源（図示せず）から供給を受けると、その後、リーダ／ライタ２からの起動コマンドを含むコマンド電文を受信するまで、一定の周期で起動コマンドを含むコマンド電文

を受信したかどうかの判定を行なう（Ｓ４０１）。データキャリア１０は、リーダ／ライタ２からの起動コマンドを含むコマンド電文を受信すると、図６のレスポンス電文フォーマットに従いレスポンス電文を作成し、作成したレスポンス電文をリーダ／ライタ２へ送信する（Ｓ４０２）。次に、リーダ／ライタ２が送信してくる位置データを含むコマンド電文を受信すると（Ｓ４０３）、データキャリア１０は、このコマンド電文に対するレスポンス電文を作成し、そのレスポンス電文をリーダ／ライタ２へ送信する（Ｓ４０４）。送信後、前述の受信したコマンド電文に含まれる位置データを用いて、データテーブルから、リーダ／ライタ２の選択決定したキーデータを選択する（Ｓ４０５）。

【００４２】データキャリア１０は、これ以降、一連の通信が終了するまで、このキーデータを用いて暗号化処理された電文にてリーダ／ライタ２との通信を行なう。

【００４３】データキャリア１０は、リーダ／ライタ２から、暗号化処理されたコマンド電文を受信すると（Ｓ４０６）、暗号化処理されたコマンド電文に対し、選択決定したキーデータを用いて暗号解読処理を行ない、暗号化処理されたコマンド電文を解読する（Ｓ４０７）。次に、データキャリア１０は、暗号解読されたコマンド電文が通信終了を指示するものかどうかを判定する（Ｓ４０８）。コマンド電文が通信終了を指示するものでない場合、データキャリア１０は、暗号化処理したレスポンス電文をリーダ／ライタ２へ送信し（Ｓ４０９）、ステップＳ４０６へ戻り、次の暗号化処理されたコマンド電文を受信するまで待機をする。ステップＳ４０８において、暗号解読されたコマンド電文が通信終了を指示するものであった場合、データキャリア１０は、そのコマンド電文に対応する暗号化処理されたレスポンス電文を作成し、リーダ／ライタ２へ送信し（Ｓ４１０）、一連の通信を終了する。

【００４４】このようにして、本発明の第２の実施の形態におけるデータキャリア１０及びリーダ／ライタ２からなる非接触型データキャリアシステム１は、一連の通信毎に、暗号化処理に用いるキーデータを変えることができ、各通信毎に異なる暗号化処理を行なうことが可能となった。

【００４５】尚、本実施の形態においては、暗号化処理の動作を簡単に説明するために、一例として、前記の簡単な式、及び図２に示す様な内容のデータテーブルを用いていてきたが、式及びデータテーブルの内容は、任意に選択及び決定することができ、本実施の形態に制限されない。

【００４６】また、本実施の形態において、位置データｎの決定方法は、単純に１を加算して、特定条件が満たされるまでループさせるものであったが、乱数を発生させて行なう方法などでもよく、本実施の形態に制限されない。

【００４７】また、決定した位置データを内部メモリに記憶させ、次回通信を行なう時に同一データとならない様にすることも可能である。

【００４８】また、本実施の形態において、暗号化処理及び暗号解読処理は、コマンド電文のコマンドコード及びデータ、及びレスポンス電文のレスポンスコード及びデータに対して行なってきたが、コマンドコード及びレスポンスコード、又はデータのどちらか一方だけに処理を行なってもよく、本実施の形態に制限されない。

【００４９】また、本実施の形態において、コマンド電文及びレスポンス電文は、それぞれ図５及び図６に示されるものを用いたが、他のフォーマットを用いてもよく、本実施の形態に制限されない。

【００５０】更に、本実施の形態において、上記の式及びデータテーブルを用いた暗号化処理は、各通信毎に一度しか行なっていないが、例えば、データテーブルにｍとして、各通信毎に何回暗号化処理を行なうかを示すデータを予め記憶させておき、それに従い、暗号化処理を行なってもよい。

【００５１】

【実施例】実施の形態において、通信の方式は、電磁結合方式を採用した。

【００５２】

【発明の効果】以上説明した様に、本発明によれば、非接触型データキャリアシステムにおけるデータキャリアとリーダ／ライタとの間の通信に用いられる暗号化処理を決定づけるキーデータを、直接通信上に現すことなく指定でき、更に、一連の通信毎にキーデータを変更することにより、各通信毎に異なった暗号化処理を行なえ、通信のセキュリティーが向上した非接触型データキャリアシステムを提供することができる。

【図面の簡単な説明】

【図１】本発明の非接触型データキャリアシステムを示すブロック図である。

【図２】本発明の実施の形態において用いたデータテーブルを示す図である。

【図３】本発明の第１の実施の形態におけるリーダ／ライタの動作概略を示す流れ図である。

【図４】本発明の第１の実施の形態におけるデータキャリアの動作概略を示す流れ図である。

【図５】本発明の実施の形態において用いたコマンド電文を示す図である。

【図６】本発明の実施の形態において用いたレスポンス電文を示す図である。

【図７】本発明の第２の実施の形態におけるリーダ／ライタの動作概略を示す流れ図である。

【図８】本発明の第２の実施の形態におけるデータキャリアの動作概略を示す流れ図である。

【符号の説明】

１　非接触型データキャリアシステム

13

2 リーダ／ライタ
3 発振器
4 制御回路
5 変調回路
6 送受信回路
7 復調回路
8 ＲＯＭ
9 ユーザー回路（ＰＣ）

14

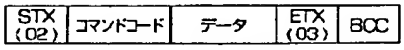
１０ データキャリア
１１ 送受信回路
１２ 復調回路
１３ 制御回路
１４ ＥＥＰＲＯＭ
１５ 変調回路
１６ ＲＯＭ

【図２】

| n | a | b |
|---|---|---|
| 0 | 15 | 34 |
| 1 | F4 | 8B |
| 2 | 2A | E5 |
| 3 | 36 | AA |
| 4 | B3 | 4C |
| 5 | AC | 03 |
| 6 | 60 | C2 |
| 7 | 9E | 44 |
| 8 | 71 | F2 |
| 9 | D0 | D6 |
| A | 81 | 15 |
| B | F2 | 9C |
| C | 24 | 89 |
| D | 8B | 27 |
| E | C2 | B1 |
| F | 05 | 8F |

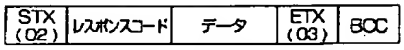
データテーブル

【図５】



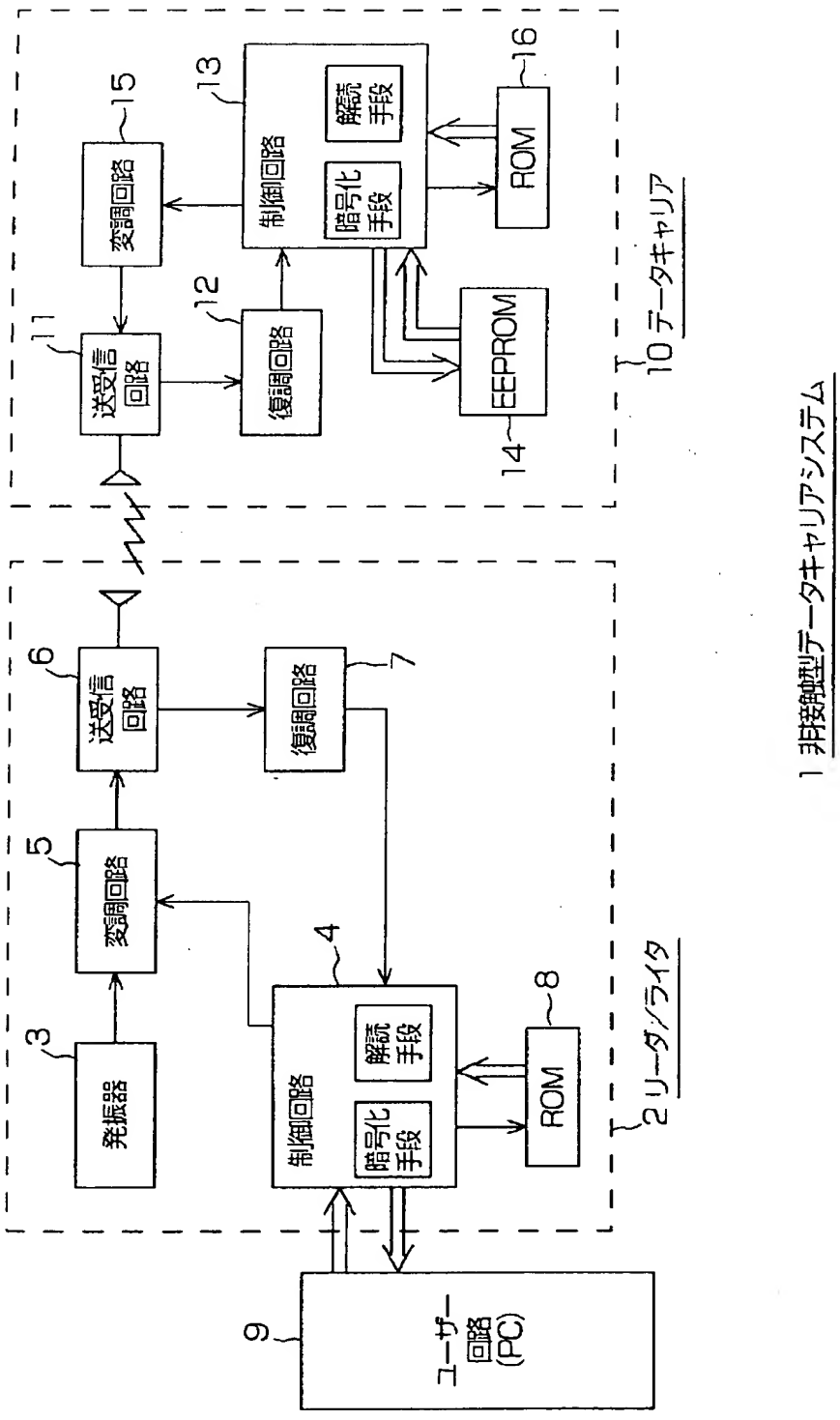

リーダ／ライタ　コマンド電文フォーマット

【図６】



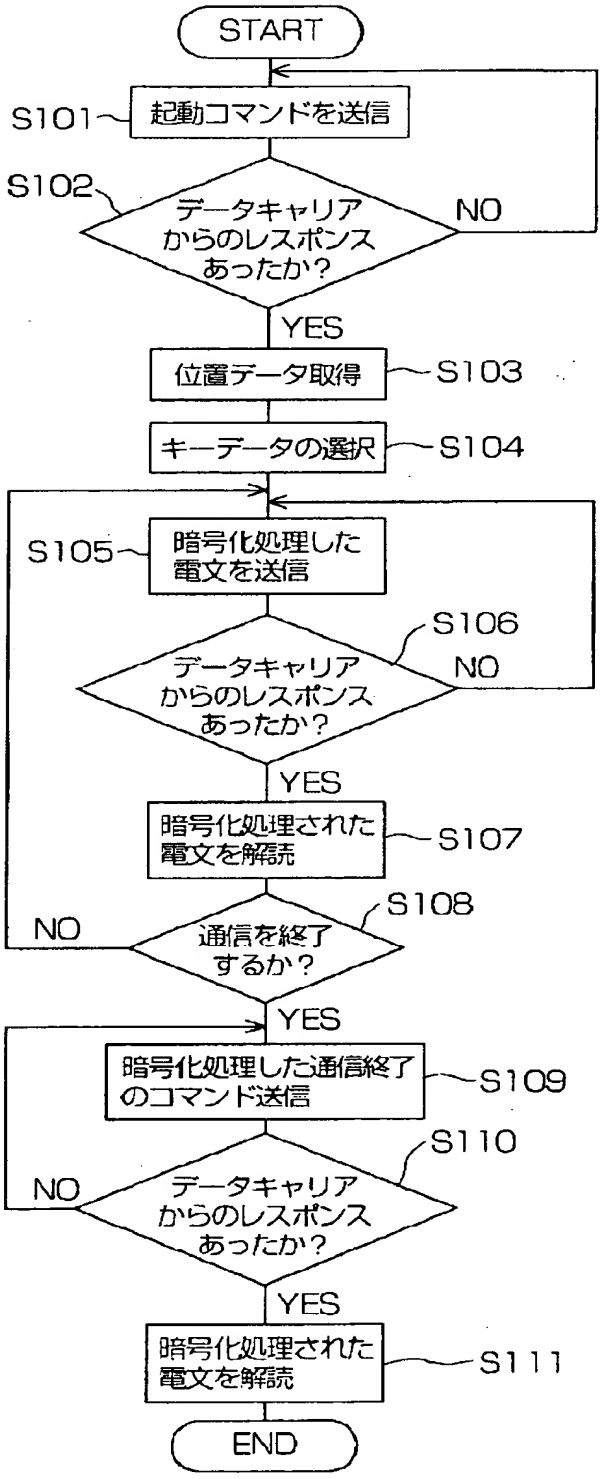

データキャリア　レスポンス電文フォーマット

【図1】


1 非接触型データキャリアシステム
2 リーダ/ライタ
10 データキャリア
3 発振器
5 変調回路
6 送受信回路
7 復調回路
4 制御回路
解読手段
暗号化手段
8 ROM
9 ユーザー回路(PC)
11 送受信回路
12 復調回路
13 制御回路
解読手段
暗号化手段
15 変調回路
16 ROM
14 EEPROM

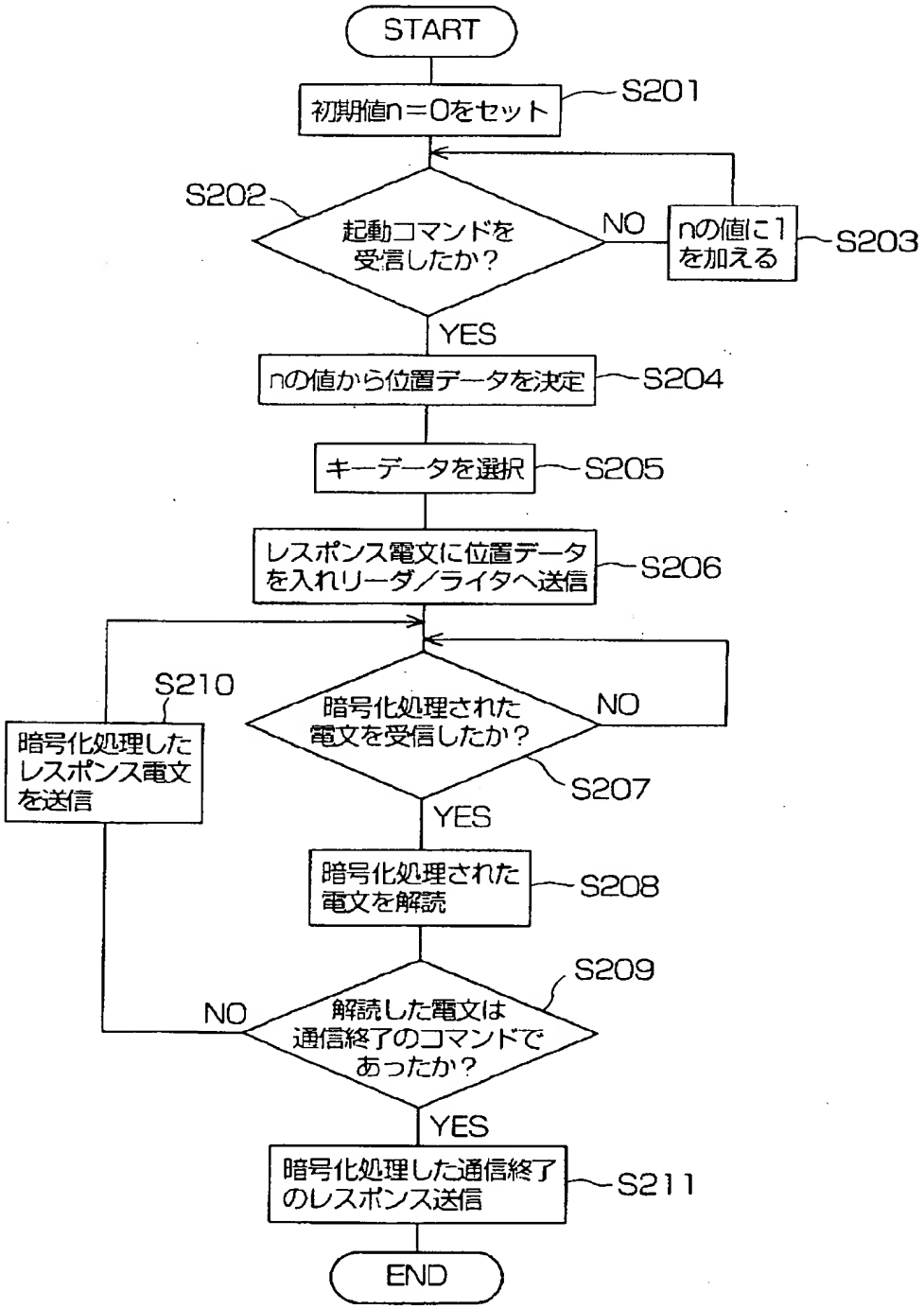
【図3】

データキャリアが位置データを決定する場合の
リーダ／ライタの動作概略フローチャート



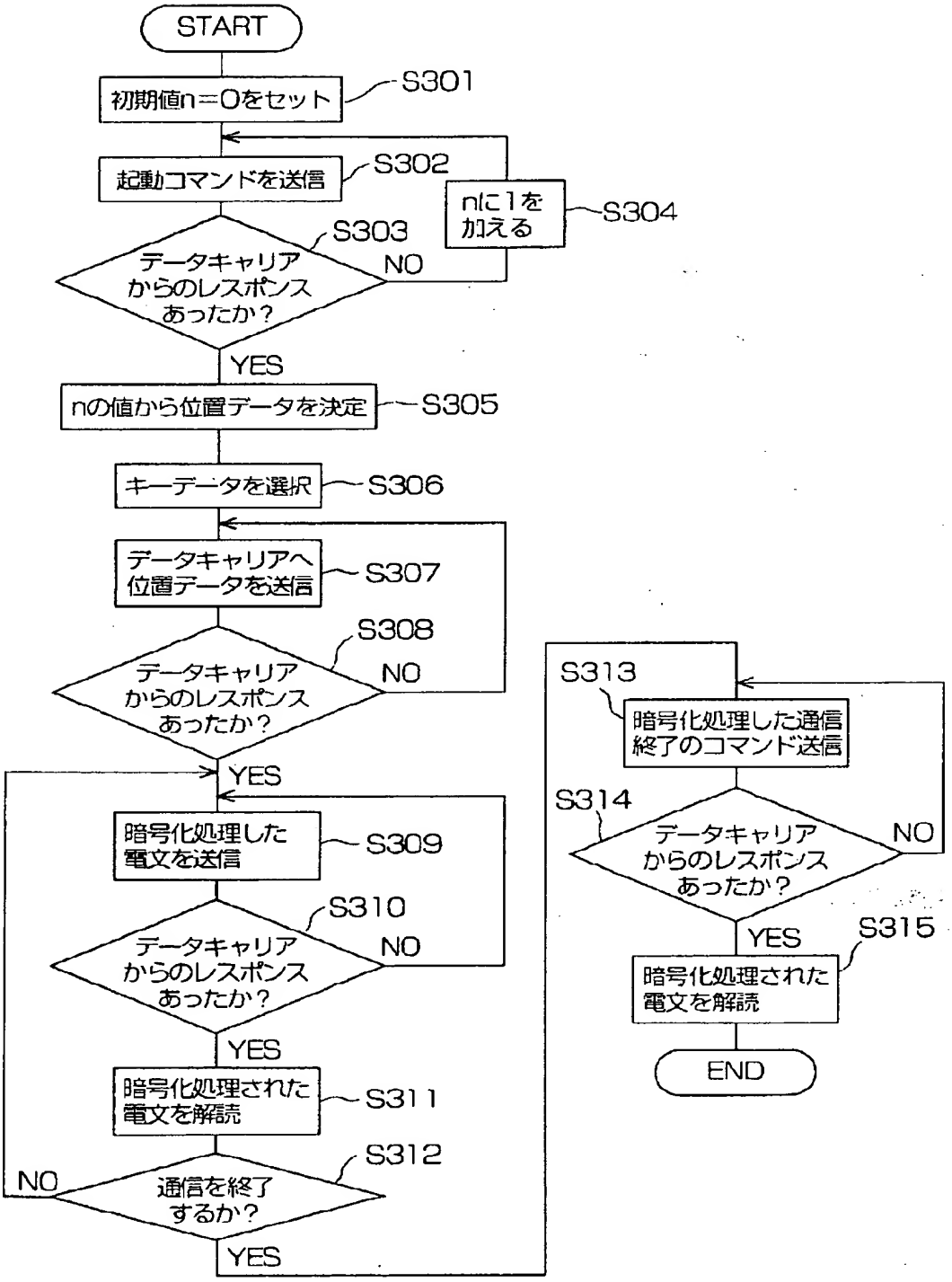
【図4】

データキャリアが位置データを決定する場合の
データキャリアの動作概略フローチャート



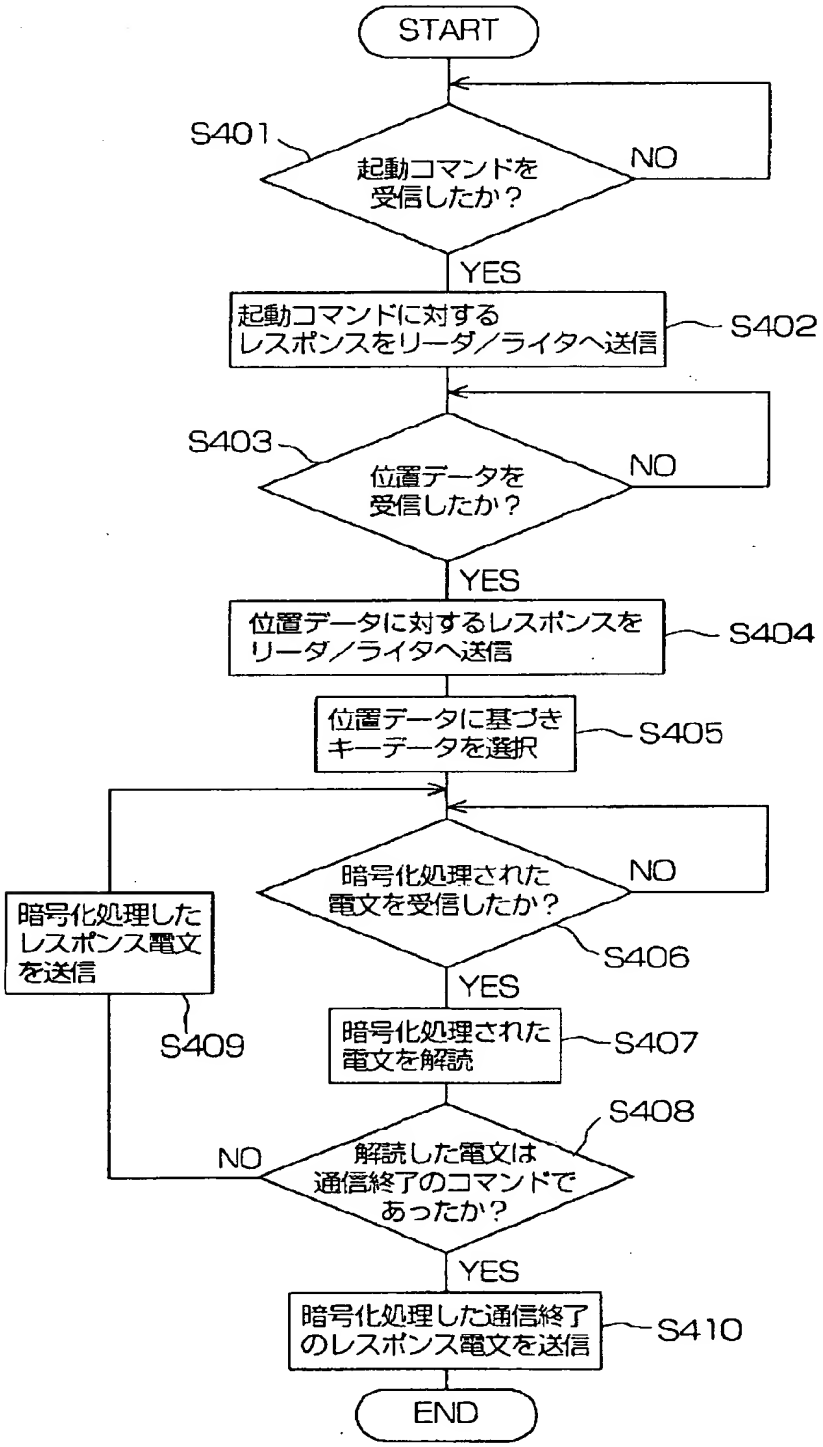
【図7】

リーダ／ライタが位置データを決定する場合の
リーダ／ライタの動作概略フローチャート



【図8】

リーダ／ライタが位置データを決定する場合の
データキャリアの動作概略フローチャート



フロントページの続き

| (51)Int.Cl.[6] | 識別記号 | 庁内整理番号 | FI | | 技術表示箇所 |
|---|---|---|---|---|---|
| H04L 9/18 | | | H04L 9/00 | 651 | |
| 12/28 | | | 11/00 | 310B | |